۱۔RATs (remote administrative tools)

یہ ایک قسم کا ٹروجن/سپائی وئیر(جاسوسی سافٹوئیر) ہے یا عام سادہ زبان میں وائرس بھی کہہ سکتے ہیں۔یہ ایک ایسا جاسوسی سافٹوئیر ہے جس میں حملہ دشمن اس کو آپ کے کمپیوٹر میں ڈلوا کر انٹرنیٹ کے ذریعے آپ کے کمپیوٹر کو استعمال کر سکتا ہے، یعنی اس میں آپ کی فائلز وغیرہ کو دیکھ سکتا ہے آپ کے لیپ ٹاپ کے ویب کیم(کیمرہ)کو کھول سکتا ہے یعنی آپ کے کمپیوٹر سے کچھ بھی کر سکتا ہے اور آپ کو بالکل معلوم بھی نہیں ہوگا۔اور ان میں ہزاروں فنکشن ہوتے ہیں ممکن ہے جس وقت آپ نیٹ استعمال کر رہے ہیں اس وقت وہ استعمال نہیں کر رہا ہوتا، اور جس وقت وہ استعمال کر رہا ہوتا ہے اس وقت آپ استعمال نہیں کر رہے ہوتے تو وہ اس سافٹوئیر کے مختلف آپشن کو سیلیکٹ کرسکتا ہے مثلاً اس آپشن پہ رکھتا ہے کہ آپ کے کمپیوٹر کی اسکرین شاٹ ہر ۱۰ منٹ بعد لیتا رہے اور جب آپ کے پاس نیٹ موجود ہو تو اس وقت انٹرنیٹ کے ذریعے دشمن پہ بھیج دے، اور بھی کئی ایسے فنکشن کے ساتھ یہ سافٹوئیر آتے ہیں۔

مگر یہ جاسوسی سافٹوئیر خود بخود نہیں آتے اِن کو حملہ کرنے والا آپ کی کمپیوٹر تک کسی نہ کسی ذریعے سے پہنچاتا ہے اور انسٹال کر واتا ہے۔ اور یہ طریقے مختلف ہوسکتے ہیں

مثلاً USB میں ڈال کر اور یو ایس بی کو آٹو رن پہ رکھا ہو یعنی جیسے ہی آپ اس کی دی ہوئی یو ایس بھی ڈالینگے فوراً سے یہ سافٹوئیر انسٹال ہوجائیگی اور خفیہ طور پر چل رہا ہوگا

دوسرا طریقہ وہ یہ کہ وہ آپ کو کوئی لنک بھیجے گا کہ اس لنک میں بہت اہم معلومات ہیں جب آپ اس کو ڈاونلوڈ کر کے اس پہ کلک کرینگے تو یہ سافٹوئیر انسٹال ہوجائگا اور خفیہ طور پر چل رہا ہوگا، اور اپنا کام شروع کر دیگا۔

اور اس کو بھیجنے کے وہ مختلف حیلے نکال سکتا ہے،مقصد اس کا آپ سے اس لنک کو کلک کروانا ہی ہے چاہے جونسا بھی طریقہ استعمال کرے۔ ویسے بازار میں سی ڈی اور ڈی وی ڈی میں بھی ان کو ڈال سکتے ہیں اور اکثر ایسا ہوتا بھی ہے کہ سی ڈیز میں ایسے سافٹوئیر پائے گئے ہیں۔

-——————

یہ صرف کمپیوٹر نہیں بلکہ اینڈرائڈ موبائل کے لئے بھی ایسے سافٹوئر آئے ہیں جن میں موبائل کی جاسوسی کی جاسکتی ہے، موبائل کے میسجز، واٹس ایپ وغیرہ کے میسیجز، کال سننا، کنٹیکٹس دیکھنا وغیرہ اس میں ممکن ہے۔اور اس کا بھیجنے کا طریقہ مختلف ہے کمپیوٹر والے سے ، اس میں حملہ کرنے والا آپ کو کوئی گیم یا ایپ کا لنک بھیجے گا یا ویسے آپ کو

دیگا اگر آپ کا کوئی اپنا ہو، اور اسی گیم یا ایپ کے ساتھ وہ اپنا یہ جاسوسی سافٹوئیر ملاتا ہے اور جب آپ اس گیم کو انسٹال کرینگے تو یہ جاسوسی سافٹوئیر خود بخود انسٹال ہوگا۔اور اپنا کام شروع کر دیگا۔ پھر اس گیم کو نکالنے سے یہ نہیں نکلتا بلکہ یہ بالکل الگ ہوتا ہے، صرف انسٹال کروانے کے کیلئے کسی گیم کے ساتھ ملاتے ہیں تاکہ لوگوں کو آسانی سے شکار بنا سکیں۔مثلاً کوئی آپ کو کوئی گیم دیگا کہ یہ ڈال دو بہت اچھی گیم ہے، جب آپ اسے ڈالینگے تو آپ کو تو معلوم نہیں ہوگا کہ اس کے ساتھ بھی کوئی چیز انسٹال ہوئی ہے یا نہیں اور گیم بھی صحیح چلتی ہے اور کسی بھی قسم کا شک بھی نہیں ہوتا۔

ریٹس سے بچنے کا طریقہ:

کسی بھی سافٹوئیر کو بغیر جانے انسٹال نہ کریں۔

کسی بھی انجان بندے کے بھیجے ہوئے لنک کو کلک مت کریں۔

بازاری سی ڈیز اور ڈی وی ڈیز سے اجتناب کریں۔

اکثر سافٹوئیر کو ڈاونلوڈ کرنے کے لئے ایک دوسرے انسٹالر کو ڈانلوڈ کر کے اس سے ا س سافٹوئیر کو ڈاونلوڈ کیا جاتا ہے ، ایسے انسٹالر سے اجتناب کریں۔

براوزر میں ایڈ بلاک پلگ اِن ضرور ڈالیں۔

یو ایس بی آٹو پلے یا آٹو رَن کا آپشن بند کریں۔

نوٹ: اس کو بند کرنے کا طریقہ اِس ٹٹورئیل کے آخر میں بتایا ہے۔ وہاں ملاحظہ فرمائیں ۔

آخری اور سب سے ضروری چیز ایک اچھا اینٹی وائرس ضرور ڈالیں ۔ہمارے مطابق بہترین اینٹی وائرس بِٹ ڈیفینڈر /Bit Defender ہے۔

مگر چونکہ ریٹس (جاسوسی سافٹوئیر) بھی اپڈیٹ ہوتے رہتے ہیں اور ان کو ایسا بنایا جاتا ہے کہ اینٹی وائرس اس کو نہ پکڑ سکیں۔ یہ ایک قسم کا مقابلہ ہے ٹروجن/ریٹس اور اینٹی وائرس کے درمیانکہ ان جاسوسی سافٹوئیرز کو ہیکرز ایسا بناتے ہیں کہ اینٹی وائرس ان کو پکڑ نہ سکیں لیکن پھر اینٹی وائرس بھی اپڈیٹ ہوتے ہیں جن میں نئے ٹروجن کو اینٹی وائرس پکڑے اور ختم کر سکیں۔

آپ خبروں میں دیکھتے ہونگے کہ فلاں اینٹی وائرس نے ایسا ٹروجن پکڑا ہے جس سے لاکھوں کمپیوٹر متاثر ہوئے ہیں، اور یہ ٹروجن فلاں ملک سے پھیلا ہے۔ یعنی ایک ملک کے ہیکرز دوسرے ملک کی جاسوسی انہی سافٹوئیڑ/ٹروجن/ریٹس سے کرتی ہے۔اور وہ مکمل FUD یعنی فُلی اَن ڈیٹیکٹ ایبل یعنی اس کو کوئی بھی اینٹی وائرس نہیں پکڑ سکتی۔ مگر پھر کوئی نہ کوئی اینٹی وائرس جب اس کا سراغ لگاتی ہے تو وہ دوسرا بناتے ہیں۔ مگر یہ وہ ریٹس ہیں جو ایک ملک دوسرے ملک کی جاسوسی کیلئے

بناتا ہے۔ اور یہ کافی بڑے لیول کا کام ہوتا ہے۔
باقی جو عام ریٹس ہیکرز نے عوام کیلئے بنائی ہیں ان کو یہ اینٹی وائرس پکڑتے ہیں، مگر وہ دوسرا نئیا ورشن بناتے ہیں اس طرح یہ سلسلہ جاری ہے۔

اس لئے اپنے اینٹی وائرس کو اَپ ڈیٹ کرتے رہیں۔

اینڈرائیڈ موبائل والے اس طرح اس سے بچ سکتے ہیں کہ کسی بھی اجنبی سے کوئی گیم وغیرہ نہ لیں۔

ویسے تو اس کا ایک ہی حل یہی ہے کہ آپ صرف اور صرف گوگل پلے اسٹور سے چیزیں ڈاونلوڈ کریں باقی کسی بھی جگہ سے ڈاونلوڈ کرنے سے شبہ ہے کہ اس میں کوئی دوسرے ملک والے نے اس میں ڈال کر بھیجا ہو۔
گوگل پلے اسٹور مکمل سیکیور ہیں۔

دوسرا آپ اچھا سا اینٹی وائرس بھی ڈالیں۔

ایک بات اس ضمن میں یہ بھی بتانا چاہونگا جو پہلے بھی کہی تھی کہ جو ایپ یا گیم آپ ڈالتے ہیں تو اس میں وہ مختلف پرمیشن مانگتا ہے، جس میں آپ کے میسیجز، کنٹیکٹس، لوکیشن وغیرہ شامل ہوتے ہیں، حالانکہ گیم کیلئے ان پرمیشن کا کوئی سروکار ہی نہیں اصل میں ہوتا یہ ہے کہ ان گیمز میں ایڈز(اشتہار) ہوتے ہیں جو ان گیم کے کمپنی کو پیسے دیتے ہیں اور یہ گیمز ان ایڈورٹائزمنٹ والے کو ان کے ڈیٹا فراہم کرتے ہیں یعنی یہ گیم آپ کیلئے مفت ہے مگر اس کے بدلے میں وہ آپ ہی کا سودا کر رہا ہوتا ہے، ضروری نہیں کہ سب ایسا کرتے ہیں لیکن کچھ ایسا کرتے ہیں۔
جیسا حال ہی میں خبر آئی تھی کہ AVG اینٹی وائرس اپنے صارفین کی ڈیٹا حاصل کر کے اپنے ایڈز/ایڈورٹائزمنٹ والے کمپنیوں کو بیچتی ہے۔ اور یہی بات تنبیہ کے طور پر لکھی تھی کہ کسی بھی چیز کو مفت نہ سمجھیں،

عام مشہور ریٹس یہ ہیں:

Xtreme Rat
DarkComet
CometRat
NJ rat
Pandroa rat
CyberGate
BlackShades
Novalite

اور اینڈرائڈ کا فی الحال ایک ہی ریٹ زیادہ مشہور ہے۔
Droid jack

اور حال ہی میں ایک خبر آئی تھی کہ پاکستانی حکومت نے ایکدوسرے ملک کے ہیکنگ ٹیم سے اس طرح کا ایک ریٹ/ٹروجن بنوایا ہے اور کروڑوں روپے میں اس کو خریدا ہے۔ اس لئے اب ہمیں محتاط ہونا ہوگا ظاہر سی بات ہے اس نے یہ اینڈیا کی جاسوسی کیلئے تو نہیں بلکہ اپنے عوام ہی کی جاسوسی کیلئے خریدا ہے۔

۲۔ Keyloggers/کی لوگرز

یہ بھی ایک قسم کا ریٹ/ٹروجن ہے، مگر اس کا کام صرف ایک ہے وہ یہ کہ یہ صرف آپ کے کی بورڈ کی جاسوسی کرتا ہے کہ آپ کیا کیا لکھ رہے ہیں، آپ کی تمام لکھائی کی جاسوسی کرتا ہے اور حملہ کرنے والے پہ بھیجتا ہے۔ آج کل نئے فنکشن کے ساتھ آرہے ہیں جس میں یہ ہوتا ہے کہ جب آپ فیس بُک یا کوئی دوسرا اکاونٹ کھول رہے ہوں ان کی جاسوسی کرے وغیرہ۔یعنی کام پھر بھی وہی آپ کی ٹائپنگ کی جاسوسی ہی ہے۔ یہ فنکشن دوسرے ریٹس میں بھی ہیں مگر چونکہ اس کی لوگر کا کام محدود ہے اور اپنے خاص کام کی وجہ سےاس کا الگ نام ہے اس لئے اس کو الگ لکھنا مناسب سمجھا۔ باقی اس کے بھیجنے کا طریقہ اور بچنے کا طریقہ وہی ہیں جو اوپر بتا چکا ہوں۔

USB ، CDs، یا دیگر میموری کارڈ وغیرہ کے آٹو پلے کو بند کرنے کا طریقہ: چونکہ ہر ونڈوز میں اُس کا طریقہ مختلف ہے اس لئے ہم یہاں ایسا طریقہ بتائینگے جو ونڈوز 98 سے لیکر ونڈوز 10 تک کام کرے۔ اور وہ ریجسٹری میں تبدیلی سے ہوتا ہے۔ اس کیلئے:

۱۔ سب سے پہلے Start پہ کلک کریں او ر وہاں Run پہ کلک کریں، ونڈوز 8 اور اس سے اوپر والے Start پہ کلک کریں یعنی ونڈوز کے نشان پہ کلک کریں چاہے کمپیوٹر میں یا کی بورڈ میں، پھر اس میں سرچ پہ کلک کریں۔

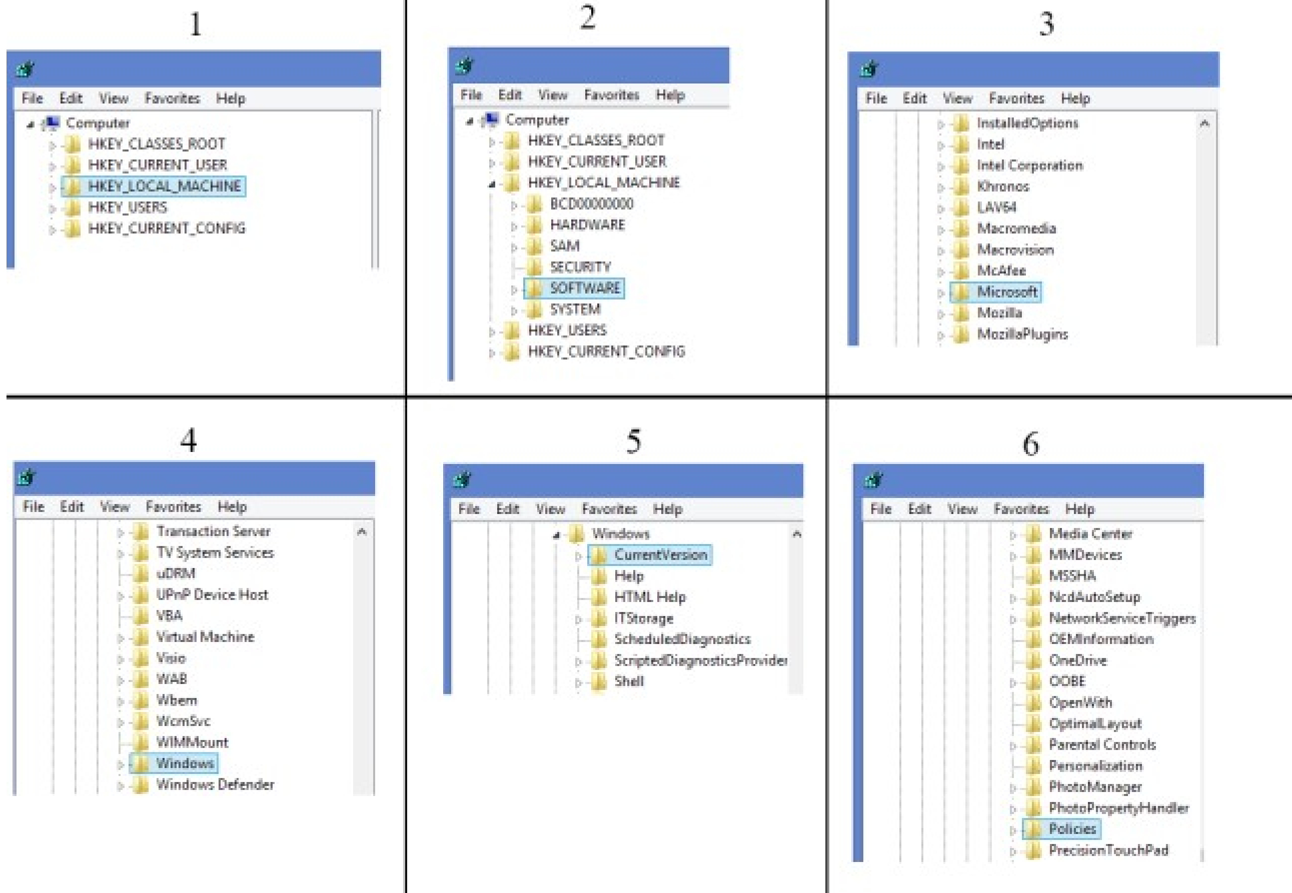
۲۔ اب رَن یا سرچ میں regedit لکھیں اور اس نام والے کو کھولیں۔

۳۔ پھر اس میں HKEY_LOCAL_MACHINE پہ ڈبل کلک کریں۔

۴۔ پھر اس فولڈر کے اندر Software کو ڈبل کلک کریں۔پھر اس میں Microsoft کو ڈبل کلک کریں۔پھر اس میں windows کو ڈبل کلک کریں۔ پھر اس میں CurrentVersion کو ڈبل کلک کریں۔ پھر اس میں policies پہ ڈبل کلک کریں۔جیسا نیچے تصویر میں دکھایا ہے۔

یعنی:

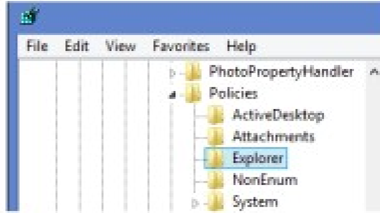
HKEY_LOCAL_MACHINE =>Software=>Microsoft=>windows=>CurrentVersion=>policies



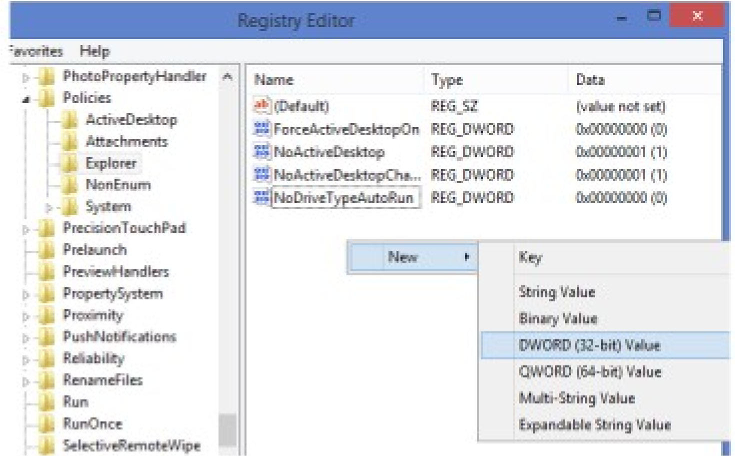
۵□ پھر Policies میں Explorer پ□ کلک کریں□دائیں طرف اس ک□
ریجسٹری ظا□ر □ونگ□□

۶□ اُس میں دیکھیں ک□ NoDriveTypeAutoRun نامی ریجسٹری/فائل
موجود □□ یا ن□یں□ اگر ن□یں □□ تو بنا لیں□ اس کیلئ□ دائیں طرف وال□
خان□ میں رائٹ کلک کریں اور new پ□ جائیں اور اس میں DWORD پ□ کلک
کریں□اور اس کو نام دیں NoDriveTypeAutoRun کا جیسا نیچ□ تصویر
میں دکھایا □□□

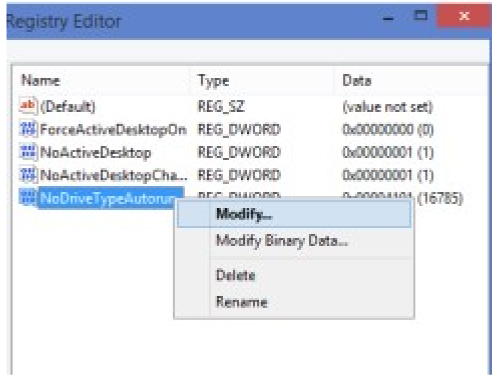
1



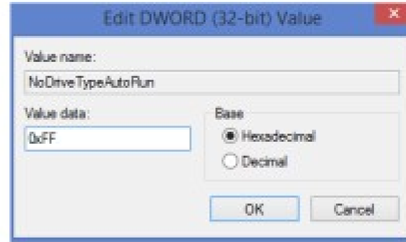
2



3



4



۷۔ اگر پہلے سے اس نام کا موجود ہے یا اب بنایا ہے دونوں صورتوں میں آپ اُس NoDriveTypeAutoRun پہ رائٹ کلک کریں اور Modify پہ کلک کریں۔

۸۔ پھر اس کے value data میں 0xFF لکھیں اور Ok پہ کلک کریں ۔ کمپیوٹر ری اسٹارٹ کریں، اب تمام ڈرائیو کے آٹو رَن/پلے بند ہوجائینگے۔

ونڈوز 8,8.1 وغیرہ میں اس کا آسان متبادل طریقہ:

آپ سیٹنگز میں جائیں، پھر Change PC Settings میں جائیں اور پھر PC and Devices اور پھر اس میں Autoplay اور اس کو Off کردیں۔

نوٹ: پھر جب بھی یو ایس بی لگائیں تو اس کے ڈرائیو کو کبھی ڈبل کلک نہ کریں، بلکہ رائٹ کلک کر کے اوپن کریں، کیونکہ اگر اس میں کوئی ٹروجن یا وائرس وغیرہ ہو تو ڈبل کلک سے بھی آٹو رَن ہو کے انسٹال ہوگا۔